



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/634,872	08/06/2003	Dani Dariel	246/211	7623
7590	06/22/2005		EXAMINER	
DR. MARK FRIEDMAN LTD C/o Bill Polkinghorn Discovery Dispatch 9003 Florin Way Upper Marlboro, MD 20772			SONG, HOSUK	
			ART UNIT	PAPER NUMBER
			2135	
			DATE MAILED: 06/22/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/634,872	DARIEL, DANI	
Examiner	Art Unit		
	Hosuk Song	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 04 April 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-54 is/are pending in the application. *Canceled*
4a) Of the above claim(s) 9, 12, 13, 22, 23 and 40 is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-8, 10-11, 14-21, 24-39, 41-54 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 06 August 2003 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a))

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1-6,10-11,14,17-21,24-25,28-31,33-34,36-39,41-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis(US 5,825,879) in view of Kihara et al(US 6,212,097).

Claim 1: Davis discloses a processor requesting encrypted digital data and decrypting the encrypted digital data, thereby providing decrypted digital data in (fig.3,5). Davis discloses a player for transforming decrypted digital data to analog signals in (col.4,lines 56-67;col.5,lines 1-4). Davis does not specifically disclose a flash memory for storing encrypted digital data. Kihara disclose this limitation in (col.9,lines 39-42). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ flash memory as taught in Kihara with system of Davis because flash memory provides low power consumption and quick speed of memory erasure which enhances overall data processing.

Claim 2: Davis disclose encrypted digital data is requested from a server and wherein requesting of encrypted digital data includes authenticating the integrated circuit to server in (fig.4 and col.3,lines 33-43).

Claim 3: Davis discloses integrated circuit is tamper-resistant in (col.4,lines 43-48).

Claims 4-5: Davis discloses encrypted digital data are video data in (col.6,lines 51-58).

Claim 6: Davis discloses processor includes an interface for receiving encrypted digital data in (fig.3).

Claim 10: Davis discloses transmitting a request for encrypted digital data from processor and for receiving encrypted digital data in (fig.2; col.4,lines 25-31).

Claim 11: Davis discloses a display device mechanism for displaying analog signals in (col.5,lines 1-4).

Claim 14: Davis discloses a single processor in (fig.3).

Claim 17: Davis discloses a server for storing the digital data in an encrypted form in (col.3,lines 39-42). Davis discloses a processor for requesting encrypted digital data from server and decrypting encrypted digital data thereby providing decrypted digital data in (fig.2). Davis discloses a player for transforming decrypted digital data to analog signals in (col.4,lines 56-67). Davis does not specifically disclose a flash memory for storing encrypted digital data. Kihara disclose this limitation in (col.9,lines 39-42). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ flash memory as taught in Kihara with system of Davis because flash memory provides low power consumption and quick speed of memory erasure which enhances overall data processing.

Claim 18: Davis disclose encrypted digital data is requested from a server and wherein requesting of encrypted digital data includes authenticating the integrated circuit to server in (fig.4 and col.3,lines 33-43).

Claim 19: Davis discloses integrated circuit is tamper-resistant in (col.4,lines 43-48).

Claim 20: Davis discloses a transceiver for transmitting to server for encrypted digital data and for receiving encrypted digital data in (col.4,lines 24-31).

Claim 21: Davis discloses a display device mechanism for displaying analog signals in (col.5,lines 1-4).

: Claim 24: Davis discloses integrated circuit includes a single processor in (fig.3).

Claim 25: Davis discloses transmitting substantially only encrypted digital data to user platform in (col.4,lines 49-55).

Claim 28: Davis discloses a processor operative to request the encrypted digital data from the server and decrypt the encrypted digital data thereby providing decrypted digital data in (fig.2;col.3,lines 39-43). Davis discloses a player operative to transform decrypted digital data to analog signals in (col.5,lines 1-4). Davis disclose requesting the encrypted digital data from the server by processor;decrypting the encrypted digital data by processor thereby providing decrypted digital data and transforming decrypted digital data to analog signals by player in (col.4,lines 49-67). Davis does not specifically disclose a flash memory for storing encrypted digital data. Kihara disclose this limitation in (col.9,lines 39-42). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ flash memory as taught in Kihara with system of Davis because flash memory provides low power consumption and quick speed of memory erasure which enhances overall data processing.

Claim 29: Davis discloses authenticating integrated circuit to the server in (fig.4 and col.3,lines 33-43).

Claim 30: Davis discloses authenticating is effected using an asymmetrical algorithm in (col.3,lines 1-2).

Claim 31: Davis discloses asymmetrical algorithm is a RSA algorithm in (col.3,lines 1-2;col.6,lines 39-42).

Claim 33: Davis discloses decrypting is effected using a symmetrical algorithm in (col.3,lines 16-18).

Claim 34: Davis disclose symmetrical algorithm is a DES algorithm in (col.3,lines 4-5).

Claim 36: Davis discloses requesting at least one key from the server by processor in (col.7,lines 1-3).

Claims 37-38: Davis does not disclose storing at least one key in a nonvolatile and encrypting at least one key prior to storing of at least one key in nonvolatile memory. Kihara disclose this limitation in (col.9,lines 39-46). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ nonvolatile memory and encrypting the key as taught in Kihara with system of Davis so that keys can be protected at all times such as against power failure.

Claim 39: Davis disclose configuring the server to send substantially only encrypted digital data and at least one key to integrated circuit in (col.4,lines 49-55).

Claim 41: Davis does not specifically disclose resetting integrated circuit. It would have been obvious to person of ordinary skill in the art to modify the invention of Davis to reset the integrated circuit in order to place the circuit back to secure mode after tamper detection such that IC can be protected against tampering.

Claim 42: Davis discloses configuring the server to send substantially only encrypted digital data to integrated circuit in (col.4,lines 49-55).

Claims 43-46: Davis discloses digital data are audio data and video in (col.4,lines 49-52). Note that MPEG is a coding of moving pictures and associated audio for digital storage media.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 47-49 are rejected under 35 U.S.C. 102(e) as being anticipated by Tagawa et al(US 6,636,773).

Claims 47-49: Tagawa disclose requesting only encrypted digital audio data and decrypting encrypted digital audio data, thereby providing decrypted digital audio data and a player for transforming decrypted digital audio data to analog signals in (col.11,lines 54-55;col.12,lines 11-14).

3. Claims 50-51,53-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis(US 5,825,879).

Claims 50,51: Davis discloses a processor requesting encrypted digital data and decrypting the encrypted digital data, thereby providing decrypted digital data in (fig.3,5). Davis discloses a player for transforming decrypted digital data to analog signals in (col.4,lines 56-67;col.5,lines 1-4). Davis discloses at least one sensor for detecting an attempt to hack at least one key in (col.4,lines 32-48).

Claims 53,54: Davis discloses a processor operative to request the encrypted digital data from the server and decrypt the encrypted digital data thereby providing decrypted digital data in (fig.2;col.3,lines 39-43). Davis discloses a player operative to transform decrypted digital data to analog signals in (col.5,lines 1-4). Davis discloses requesting the encrypted digital data from the server by processor; decrypting the encrypted digital data by processor thereby providing decrypted digital data and transforming decrypted digital data to analog signals by player in (col.4,lines 49-67). Davis discloses storing received encrypted digital data in a memory separate from integrated circuit by the processor in (fig.2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis(US 5,825,879) in view of Kihara et al(US 6,212,097) and further in view of Dlugosch(US 6,789,146)

Claims 7-8:Neither Davis nor Kihara specifically disclose interface is selected from the group consisting of an ISO7816 interface,a local bus interface,MMCA interface, a SDA interface,a USB interface and a parallel interface. Dlugosch disclose this limitation in (col.4,lines 1-15 and table I). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ selected interface as taught in Dlugosch with system of Davis and Kihara to enhance and improve data processing scheme.

4. Claims 15-16,26-27,26-27,32,35,52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis(US 5,825,879).

Claim 15-16,26-27: Official notice is taken that management code is stored only in ROM is well known in the art. One of ordinary skill in the art would have been motivated to store management code in ROM in order to prevent illegal modification thus preventing intrusion.

Claim 32: Davis does not specifically disclose ECC algorithm. It would have been obvious to person of ordinary skill in the art at the time invention was made to employ ECC algorithm because ECC device require less storage,less power,less memory and less bandwidth than other systems and provides enhanced data security.

Claim 35: Official notice is taken that Rijndael algorithm is well known in the art. One of ordinary skill in the art would have been motivated to employ Rijndael algorithm because of its new generation symmetric block cipher that supports key sizes up to 256 bits for enhanced security.

Claim 52: Davis discloses a processor operative to request the encrypted digital data from the server and decrypt the encrypted digital data thereby providing decrypted digital data in (fig.2;col.3,lines 39-43). Davis discloses a player operative to transform decrypted digital data to analog signals in (col.5,lines 1-4). Davis disclose requesting the encrypted digital data from the server by processor;decrypting the encrypted digital data by processor thereby providing decrypted digital data and transforming decrypted digital data to analog signals by player in (col.4,lines 49-67). However, Davis does not specifically disclose resetting integrated circuit. It would have been obvious to person of ordinary skill in the art to modify the invention of Davis to reset the integrated circuit in order to place the circuit back to secure mode after tamper detection such that IC can be protected against tampering.

Response to Amendment

5. Applicant has amended claims 1-8,10-11,14-17,28,37-39,41-42 and added new claims 43-54. Claims 9,12-13,22-23,40 has been canceled.

The previous grounds of rejection are withdrawn in view of Applicant's Amendment filed on 4/4/05. The new grounds of rejection are presented above.

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 571-272-3857. The examiner can normally be reached on Tue-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS


Hosuk Song
Primary Examiner
Art Unit 2135